LA-UR-02-6899

Theory Component
# of the
Quantum Information Processing
and
Quantum Computing Roadmap

A Quantum Information Science and Technology Roadmap

Part 1: Quantum Computation

Section 6.8

Disclaimer:
The opinions expressed in this document are those of the Technology Experts' Panel members and are subject to change. They should not to be taken to indicate in any way an official position of the U.S. Government sponsors of this research.

December 1, 2002
Version 1.0

This document is available electronically at: http://qist.lanl.gov

Produced for the Advanced Research and Development Activity (ARDA)

Compiled by: Gary Doolen and Brigitta Whaley

Editing and compositing: Todd Heinrichs

This report was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees make any warranty, express or implied, or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof.

The United States Government strongly supports academic freedom and a researcher's right to publish; as an institution, however, the U.S. Government does not endorse the viewpoint of a publication or guarantee its technical correctness. By acceptance of this article, the publisher recognizes that the U.S. Government retains a nonexclusive, royalty-free license to publish or reproduce the published form of this contribution, or to allow others to do so, for U.S. Government purposes. The United States Government requests that the publisher identify this article as work performed under the auspices of the Advanced Research and Development Activity (ARDA).

Table of Contents

List of Acronyms and Abbreviations

1-D	one-dimensional	MRFM	magnetic resonance force microscopy
2-D	two dimensional	NMR	nuclear magnetic resonance
BEC	Bose-Einstein condensate	NP	nondeterministic polynomial (time)
BQNP	bounded quantum analogue of NP	P	polynomial (time)
BQP	bounded quantum polynomial	PSPACE	problem solvable with polynomial memory
C-NOT	controlled-NOT (gate)	QC	quantum computation/computing
DFS	decoherence-free subspace	QCPR	Quantum Computing Program Review
FQHE	fractional quantum Hall effect	QIP	quantum information processing
GHZ	Greenberger-Horne-Zeilinger	QSAT	quantum analog of satisfiable problem
IP	interaction proof	SQUID	superconducting quantum interference device
MA	Merlin-Arthur (problems)	TEP	Technology Experts Panel

1.0 Introduction

Note: This document constitutes the most recent draft of the Theoretical Approaches detailed summary in the process of developing a roadmap for achieving quantum computation (QC). Please submit any comments or suggestions on this detailed summary to Todd Heinrichs (tdh@lanl.gov) who will forward them to the relevant Technology Experts Panel (TEP) member. With your input we can improve this roadmap as a guidance tool for the continued development of QC research.

In this section of the roadmap we focus on historical aspects of quantum information theory, its role leading up to the current stage of development of QC, and examples of unanticipated advances and significant theoretical advances. The panel will revisit the theory component of the roadmap in a future version. For example, sections summarizing outstanding problems and new directions will be added.

2.0 Quantum Theory Historical Review: A short summary of significant breakthroughs in Quantum Information Theory

Information theory is rooted in physics, which places limitations on how information may be processed and manipulated for computation and for communication. Before the 1980s this meant classical physics, but since that time there has been a conscious paradigm shift to the examination of benefits that may derive from basing a theory of information upon the laws of quantum physics. At least two important precursors to this paradigm shift had critical influence. The first was the demonstration of nonlocal correlations between different parts of a quantum system, correlations that possess no classical counterpart, by Bell in the early 1960s[1]. The second important precursor to the new field of "Quantum Information Theory" was provided by the work of Landauer and Bennett on the thermodynamic cost of computation[2,3]. Bennett's 1973 proof that reversible classical computation is possible[3] was the key idea in Benioff's positive response in 1980 to negative prognoses of fundamental limitations of computation provided by physics[4].

In a key paradigm shift, Feynman pointed out in 1992 that simulating quantum physics on a classical computer appeared to incur an exponential slowdown[5], thus paving the way for quantum computation. Deutch took a major step further in 1985, with the introduction of quantum circuits and universal gate sets, providing the critical leap from the restrictions of Boolean logic underlying classical computation to nonBoolean unitary operations[6]. With this critical step, the concept of quantum computation was formalized. In 1993, Bernstein and Vazirani[7] built upon an algorithm of Deutsch and Jozsa[8], to show that quantum computers provide a superpolynomial advantage over probabilistic computers, thus showing that quantum computers violate the modified Church-Turing thesis. These algorithms as well as Simon's 1994 algorithm[9] benefited from the features of quantum superposition and entanglement, with the roots of the latter clearly identifiable with the nonclassical correlations observed by Bell in the early 1960s. This slow growth in exploration of algorithmical advantages derived from quantum circuits for computation virtually exploded in 1994 with the discovery by Shor of the polynomial time quantum algorithms for integer factorization and discrete logarithm problems [10], followed by the discovery of the quadratic speed-up quantum search algorithm by Grover in 1996 [11]. Both of these theoretical results galvanized the experimental community into active consideration of possible implementations of quantum logic. Experimental interest was further stimulated by another significant result of Calderbank, Shor, and Steane namely that error correction codes could be constructed to protect quantum states just as for classical states [12]. This demonstration of quantum error correction in 1995 was subsequently incorporated into a scheme by Kitaev [13], Shor [14], Aharonov and Ben-Or [15], Knill, LaFlamme, and Zurek [16], and Gottesman and Preskill [17,18] to provide error thresholds on individual operations that show when computation can continue successfully in the presence of decoherence and errors ('fault tolerant' computation). This result put the implementation of quantum computation on a similar footing with classical computation using unreliable gates, and significantly altered the consciousness of the physics community with regard to experimental implementation.

Quantum complexity theory systematically studies the class of problems that can be solved efficiently using quantum resources such as entanglement. Bernstein and Vazirani,s 1993 work showed that relative to an oracle the complexity class BQP, of problems that can be solved in polynomial time on a quantum computer, is not contained in MA, the probabilistic generalization of NP [7]. Thus even in the unlikely event that P = NP, quantum computers could still provide a speed-up over classical computers. The **limits** of quantum computers were explored by Bennett, Bernstein, Brassard, and Vazirani [19], who showed that quantum computation cannot speed up search by more than a quadratic factor. This showed that Grover's algorithm is optimal and that, relative to a random oracle, quantum computers cannot solve NP-complete problems. They also showed a similar lower bound for inverting a random permutation by a quantum computer, thus opening up the possibility of quantum one-way functions. Recently, Aaronson showed a similar lower bound for the collision problem [20], thus showing that there is no generic quantum attack against collision intractable hash functions. Kitaev has studied the class BQNP, the quantum analogue of NP, and showed that QSAT, the quantum analogue of the satisfiability problem is complete for this class—thus proving that BQNP□ PSPACE [13]. Watrous considered the power of quantum communication in the context of interactive proofs, and showed that the class IP of problems which have interactive proofs with polynomially many rounds of communication can be simulated with only three rounds of quantum communication [21]. In the first demonstration of the power of quantum communication, Burhman, Cleve, and Wigderson showed how two parties could decide set disjointness by communicating only square root of *n* quantum bits, quadratically fewer than the number required classically [22]. Ambainis, Schulman, Vazirani, and Wigderson showed that for the problem of sampling disjoint subsets, quantum communication yields an exponential advantage over any protocol that communicates only classical bits [23].

Similar paradigm-changing advances have occurred in the theory of data transmission and communication as a result of theoretical breakthroughs in quantum information theory. In fact the oldest branch of quantum information theory concerns the use of quantum channels to transmit classical information, with work of Holevo dating from 1973 [24]. Since then, many significant results for the use of quantum channels to transmit both classical and quantum information have been established. It is useful to realize that these, in many cases very practical, results are derived notwithstanding the two famous results concerning inaccessibility of quantum states, namely the impossibility of distinguishing distinct quantum states (Holevo) [24] and of copying (or 'cloning') an unknown quantum state (Wooters & Zurek) [25]. Notable amongst these quantum-information theoretic results with implications for practical use in quantum communication are quantum data compression, quantum superdense coding, and teleportation. Together with quantum error correction, quantum data compression provides a quantum analog for the two most important techniques of classical information theory. The developments of quantum superdense coding in 1992 (Bennett & Wiesner) [26] and quantum transmission by teleportation (Bennett & coworkers) [27] in 1993, have no classical analogue and are thus very surprising when viewed from a classical paradigm. Teleportation allows states to be transmitted faithfully from one spatial location to the other, while superdense coding allows the classical information to be transmitted with a smaller number of resources (quantum bits) via a quantum channel. A related property of quantum channels is superadditivity, namely that the amount of classical information transmitted may be increased by use of parallel channels [28,29]. Similar to the development of theoretical techniques to deal with noise in quantum computation mentioned above, a significant theoretical effort has also focused on the issues arising from communication with noisy channels. Several results have emerged here, but a number of open questions still remain and this is a very active area of theoretical work. Important results arrived at in recent years include a bound on the capacity of a noisy quantum channel for transmission of classical information (Holevo-Schumacher-Westmoreland theorem [30–32]), and the development of protocols for distillation (or 'purification') of entanglement [33–35].

A related area in which quantum information theory has made remarkable advances in the last 20 years is quantum cryptography. This field provides one of the most successful practical applications of quantum information to date, with the procedures for secure quantum key distribution (QKD). First developed by Bennett and Brassard in 1984 [36], several protocols now exist to make a provably secure quantum key for distribution over a public channel. These schemes rely on the uncertainty of distinguishing quantum states, with the security of the key also guaranteed as a result of the ability to detect any eavesdropping measurement by an observed increase in error rate of communication between the two parties. The remarkable security properties of QKD are a direct result of the properties of quantum information, and hence of the underlying principles of quantum physics.

These advances have demonstrated the usefulness, in many cases unexpected, of treating quantum states as information. They have also validated the field of quantum information theory, providing a critical stimulus to experimental investigation and in some cases literally opening the path to realization of quantum processing of information for communication or computation. In fact, several of the most nonclassical or counterintuitive of the theoretical predictions have been the first to receive experimental verification (*e.g.*, teleportation, superdense coding, and QKD). Looking back on these developments over the last 20 years, it is reasonable to expect that further investigation into the fundamentals of quantum information will continue to provide new and useful insights into issues with very practical implications. We can identify several outstanding open questions in quantum information theory today, whose solution would impact the field as a whole. These include complete analysis of channel capacities for quantum information transmitted via quantum channels and quantification of entanglement measures for many-particle systems. Another, relatively new direction in quantum information theory focuses on the use of measurements as an enabling tool for quantum information processing, rather than merely as a final step or source of decoherence. Measurement provides our limited access to the exponential resources intrinsic to quantum states, and recent work has shown that this access can itself be manipulated to control the processing, including some schemes to perform entire computations using only measurements in massively entangled states.

The exploration of new quantum algorithms has achieved some success over the last couple of years, following a lull of about six years after Shor's algorithm. These include Hallgren's 2002 quantum algorithm for Pell's equation [37] (one of the oldest problems in number theory), which breaks the Buchman-Williams cryptosystem. The framework for quantum algorithms has also been extended beyond the hidden subgroup problems. van Dam, Hallgren, and Ip's 2000 quantum algorithm for shifted multiplicative characters [38,39] breaks homomorphic cryptosystems, and the same techniques were recently extended by van Dam and Seroussi (2002) to a quantum algorithm for estimating Gauss sums [40]. The framework of adiabatic quantum algorithms introduced by Farhi, Goldman, Goldstone, and Sipser 2000 [41], and explored by van Dam, Mosca, and Vazirani 2001 [42] provides a novel paradigm for systematically designing quantum algorithms.

3.0 References

[1] Bell, J. S., "On the Einstein-Podolski-Rosen paradox," *Physics* **1**, 195–200 (1964), reprinted in *Speakable and Unspeakable in Quantum Mechanics*, (Cambridge University Press, Cambridge, UK, 1987) pp. 14–21;

Bell, J. S., "On the problem of hidden variables in quantum mechanics," *Reviews of Modern Physics* **38**, 447–452 (1966).

[2] Landauer, R., "Irreversibility and heat generation in the computing process," *IBM Journal of Research and Development* **5**(3), 183–191 (1961).

[3] Bennett, C. H., "Logical reversibility of computation," *IBM Journal of Research and Development* **17**(6), 525–530 (1973).

[4] Benioff, P., "The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines," *Journal of Statistical Physics* **22**, 563–591 (1980);

Benioff, P., "Quantum mechanical models of Turing machines that dissipate no energy," *Physical Review Letters* **48**, 1581–1585 (1982).

[5] Feynman, R. P., "Simulating physics with computers," *International Journal of Theoretical Physics* **21**, 467–488 (1982).

[6] Deutsch, D., "Quantum theory, the Church-Turing principle and the universal quantum computer," *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **400**(1818), 97–117 (1985).

[7] Bernstein, E. and U. Vazirani, “Quantum complexity theory,“ *Proceedings of the of the 25th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1993) pp. 11–20 [ISBN:0-89791-591-7].

[8] Deutsch, D. and R. Josza, “Rapid solution of problems by quantum computation,“ *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **439**, 553–558 (1992).

[9] Simon, D., “On the power of quantum computation,“ *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (FOCS 94)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1994) pp. 116–123.

[10] Shor, P. W., “Algorithms for quantum computation: discrete logarithms and factoring,“ *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science (FOCS 94)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1994) pp. 124–134; revised version at quant-ph/9508027.

[11] Grover, L., “A fast quantum mechanical algorithm for database search,“ *Proceedings of the 28th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 1999) pp. 212–219 [ISBN:0-89791-785-5, *quant-ph*/9605043].

[12] Shor, P. W., “Scheme for reducing decoherence in quantum computer memory,“ *Physical Review A* **52**, R2493–R2496 (1995);

Calderbank, A. R. and P. W. Shor, “Good quantum error-correcting codes exist,“ *Physical Review A* **54**, 1098–1105 (1996);

Steane, A. M., “Error correcting codes in quantum theory,“ *Physical Review Letters* **77**, 793–797 (1996).

[13] Kitaev, A., “Quantum computations: Algorithms and error correction,“ *Russian Mathematical Surveys* **52**, 1191–1249 (1997).

[14] Shor, P. W., “Fault-tolerant quantum computation,“ *Proceedings of the 37th Annual Symposium on the Foundations of Computer Science (FOCS 96)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1996) pp. 56–67.

[15] Aharonov, D. and M. Ben-Or, “Fault tolerant quantum computation with constant error,“ preprint *quant-ph*/9611025.

[16] Knill, E., R. Laflamme and W. H. Zurek, “Resilient quantum computation: Error models and thresholds,“ *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **454**, 365–384 (1998).

[17] Gottesmann, D., “Stabilizer codes and quantum error correction,“ Ph.D. thesis, California Institute of Technology (1997) (114 pp. - electronic version at *quant-ph*/9705052).

[18] Preskill, J., “Reliable quantum computers,“ *Proceedings of the Royal Society of London: Series A - Mathematical and Physical Sciences A* **454**, 385–410 (1998).

[19] Bennett, C. H., E. Bernstein, G. Brassard, and U. Vazirani, "Strengths and weaknesses of quantum computing," *SIAM Journal on Computing* **26**, 1510–1523 (1997).

[20] Aaronson, S., "Quantum lower bound for the collision problem," *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 2002) pp. 635–642 [ISBN:1-58113-495-9, *quant-ph*/0111102].

[21] Watrous, J., "On quantum and classical space-bounded processes with algebraic transition amplitudes," *Proceedings of the 40th Annual Symposium on the Foundations of Computer Science (FOCS 99)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1999) pp. 341–351.

[22] Buhrman, H., R. Cleve, and A. Wigderson, "Quantum vs. classical communication and computation," *Proceedings of the 30th Annual ACM Symposium on Theory of Computing,* (Association for Computing Machinery Press, New York, 1998) pp. 63–68 [ISBN:0-89791-962-9].

[23] Ambainis, A., L. J. Schulman, A. Ta-Shma, U. Vazirani, and A. Wigderson, "The quantum communication complexity of sampling," *Proceedings of the 39th Annual Symposium on the Foundations of Computer Science (FOCS 98)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 1998) pp. 342–351.

[24] Holevo, A. S., "Bounds for the quantity of information transmitted by a quantum communication channel," *Problems of Information Transmission* **9**(3), 177–183 (1973).

[25] Wooters, W. K. and W. H. Zurek, "A single quantum cannot be cloned," *Nature* **299**, 802–803 (1982).

[26] Bennett, C. H. and S. J. Wiesner, "Communication via one- and two-particle operators on Einstein-Podolsky-Rosen states," *Physical Review Letters* **69**, 2881–2884 (1992).

27] Bennett, C. H., G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters, "Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels," *Physical Review Letters* **70**, 1895–1899 (1993).

[28] Schumacher, B., M. Westmoreland, and W. K. Wootters, "Limitation on the amount of accessible information in a quantum channel," *Physical Review Letters* **76**, 3452–3455 (1997).

[29] Sasaki, M., K. Kato, M. Izutsu, and O. Hirota, "Quantum channels showing superadditivity in classical capacity," *Physical Review A* **58**, 146–158 (1998).

30] Holevo, A. S., "On capacity of a quantum communications channel," *Problems of Information Transmission* **15**(4), 247–253 (1979).

[31] Schumacher, B. and M. Westmoreland, "Sending classical information via noisy quantum channels," *Physical Review A* **56**, 131–138 (1997).

[32] Holevo, A. S., "The capacity of the quantum channel with general signal states," *IEEE Transactions on Information Theory* **IT-44**(#1), 269–273 (1998).

[33] Bennett, C. H., H. J. Bernstein, S. Popescu, and B. Schumacher, “Concentrating partial entanglement by local operations,“ *Physical Review A* **53**, 2046–2052 (1996).

[34] Bennett, C. H., G. Brassard, S. Popescu, B. Schumacher, J. A. Smolin, and W. K. Wootters, “Purification of noisy entanglement and faithful teleportation via noisy channels,“ *Physical Review Letters* **76**, 722–725 (1996).

[35] Bennett, C. H., D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, “Mixed-state entanglement and quantum error correction,“ *Physical Review A* **54**, 3824–3851 (1996).

[36] Bennett, C. H. and G. Brassard, “Quantum cryptography: Public key distribution and coin tossing,“ *Proceedings of the IEEE International Conference on Computers Systems and Signal Processing*, (IEEE, New York, 1984) pp 175–179.

[37] Hallgren, S., “Polynomial-time quantum algorithms for Pell's equation and the principal ideal problem,“ ,“ *Proceedings of the 34th Annual ACM Symposium on Theory of Computing*, (Association for Computing Machinery Press, New York, 2002) pp. 653–658 [ISBN:1-58113-495-9].

[38] van Dam, W. and S. Hallgren, “Efficient quantum algorithms for shifted quadratic character problems,“ preprint *quant-ph*/0011067.

[39] Ip, L., “Solving shift problems and hidden coset problem using the Fourier transform,“ preprint *quant-ph*/0205034.

[40] van Dam, W. and G. Seroussi, “Efficient quantum algorithms for estimating Gauss sums,“ preprint *quant-ph*/0207131.

[41] Farhi, E., J. Goldstone, S. Gutmann, and M. Sipser, “Quantum computation by adiabatic evolution,“ preprint *quant-ph*/0001106.

[42] van Dam, W., M. Mosca, and U. Vazirani, “How powerful is adiabatic quantum computation?,“ *Proceedings of the 42nd Annual Symposium on the Foundations of Computer Science (FOCS 01)*, (IEEE Computer Society Press, Los Alamitos, California, USA, 2001) pp. 279–287.